NEXTLABS®

SkyDRM for iManage

OVERVIEW

iManage helps organizations manage documents more efficiently and leverage knowledge to drive better business outcomes. However, today's business environment increasingly requires the sensitive and restricted data to be shared with globally distributed workers, customers, and external partners, often accessing information on unmanaged or managed devices. How can companies continue to leverage the benefits of using iManage for agile collaboration, but also secure the data at rest and in transit across today's extended enterprise?

Enterprise digital rights management (E-DRM) is a technology that protects sensitive enterprise information and data from unauthorized access and use. It allows for secure collaboration, sharing, viewing, editing, printing, making a copy, screen capture, extracting content, and expiration across internal and external stakeholders. E-DRM applies rules and policies to the information distributed in electronic documents and can update or revoke them even the document has been shared. E-DRM protects information against theft, misuses, or inadvertent disclosure, and mitigates the business, legal, and regulatory risks of collaboration and information exchanges with partners, customers, and across the extended enterprise.

THE SOLUTION

NextLabs SkyDRM for iManage applies Enterprise Digital Rights Management (E-DRM) to extends security and usage control to files downloaded from iManage to achieve end-to-end protection for sensitive data at rest and on the move.

SkyDRM for iManage can automatically protect valuable files at rest inside of iManage Cloud and On-Premises with security envelop using DRM. The security envelop includes security labels (i.e., client and matter) from iManage. The combination of security labels (client and matter) and user groups in IDP (e.g., Azure AD) are used to determine the rights of the users dynamically in real time to access the data. Based on the permission granted by the policy engine, authorized users can open, view, and even modify the DRM protected files using Microsoft Office and other native applications after the users check-out the files from iManage. After user modified the protected file in local drive, user can check-in the file seamlessly into iManage. Data owners get full visibility into how their data is being shared, accessed, and used at rest and in transit.

SkyDRM for iManage provides the following key capabilities:

- Automated rights protection encrypts and tags valuable files managed in iManage with predefined rules. The security labels inherit classification such as client and matter value from iManage. Protection stays with the files regardless of where those files are located and travel to - inside and outside of iManage.
- Access and usage controls over files, such as limiting access, editing, printing, copying, screen capture, and enforcing time-based rights over protected files inside and outside of iManage based on data classification (client and matter) and user's groups in IDP dynamically.

- Native integration with Microsoft Office and other 3rd party applications seamlessly on iManage client side. Enables user to open, view, and edit the protected file with native applications after user checks the protected files out of iManage if user has the proper permissions.
- Secure viewing from any device with a HTML5-compatible browser. Supported file types include Microsoft Office documents, PDF, JPG, PNG, and a variety of file formats. The viewer provides a multitude of interactive visualization capabilities like Zoom In, Zoom Out, and Rotate.
- Allow iManage Work Indexer to index the protected files in iManage with metadata contents and thumbnail image.
- Monitoring and reporting of data use to get full visibility on usage and sharing of critical data.

THE RESULT

Using SkyDRM for iManage. companies are able to:

- Automatically protect the files in iManage with client and matter security labels from iManage. Extend the protection to the downloaded/checked out files.
- Control the access and usage of the files shared with internal and external users with Microsoft Office and native applications based on the security labels (client and matter) from iManage and user's groups in IDP.
- Eliminate manual security procedures that impede collaboration.
- Allow iManage Work Indexer to scan protected files in iManage.
- Comprehensive visibility into access events and data for audit, oversight, and troubleshooting.

SOLUTION COMPONENTS

The SkyDRM for iManage is comprised of multiple integrated components selected and deployed according to the company's use case. The complete solution allows companies to securely share product data both internally with global employees and externally with collaborative partners and suppliers.

Rights Manager for iManage

The Rights Manager for iManage automatically protects sensitive files according to iManage data classification (i.e., client and matter) and access security. It integrates iManage and the SkyDRM Rights Management Server to protect (tag and encrypt) files before data is shared.

Rights Management Server

The Rights Management Server provides two functions. First, it applies rights protection to ensure only authorized people get access, and second, it provides secure viewing of protected documents from any device via any HTML5 web browser. Available either on-premise or in the cloud, Secure Viewing is well-suited for use cases where business and legal document needs to be shared with external users who are unable to install client side software or where users prefer to view the shared documents from mobile devices.

Rights Management Client

The Rights Management Client provides secure access, viewing, and editing of protected files using native applications. Unlike other rights management products, which only supports a handful of file formats and applications, the NextLabs SkyDRM product is built to support any file format and application, allowing customers to protect critical legal and business data in Office, PDF, and email files. The Rights Management Client also works completely offline, making it well-suited for mobile users in the field that needs offline access to critical documents.

Centralized Management and Reporting

SkyDRM for iManage is built on the NextLabs CloudAz Zero Trust Policy Platform, the industry leading information control policy platform for central management, control, and activity analytics. Companies can now have one set of policies for all critical legal and business documents across iManage and various document management systems with centralized visibility to quickly highlight unusual access patterns or behavior - to prevent breaches, misuse, and violations.

Feature	SUPPORT
Supported File Formats in Viewer	Microsoft Word, Microsoft PowerPoint, Microsoft Excel, Microsoft Visio, Adobe PDF, Source code (java, cpp, xml, html, etc.), Picture file (jpg, png, tif, bmp, etc.), CAD (MicroStation, AutoCAD, SolidWorks, Creo, CATIA, Parasolid, NX, Solid Edge, Siemens JT), SAP Visual Enterprise (Web Viewer only), Common CAD formats (dgn, dwg, igs, iges, stp, stl, step, etc.), and many more
Supported Controls	View (Access Control), Edit, Print, Re-Share, Save As (Make a Local Copy), Screen Capture, Extract (Make a Decrypted Copy), Watermark, Expiration
Container Platform	Kubernetes
Server Platforms	Docker CE, RHEL, Ubuntu, Windows
Supported Clients	HTML 5 Browsers (Edge, Chrome, Safari, Firefox), Windows, iOS
Supported Identity Providers	Azure AD, Active Directory (AD), Okta, Active Directory Federation Services (ADFS), OneLogin, PingOne, SAML IdP, OAuth IdP, etc.
Supported Cloud and SaaS Apps	Google Drive, OneDrive, SharePoint Online, SharePoint On-Premises, Dropbox
RMX for Enterprise Applications	Microsoft Office, SharePoint, SharePoint Online, Siemens Teamcenter, Bentley ProjectWise, SAP ERP

ABOUT NEXTLABS

NextLabs®, Inc. provides zero trust data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based zero trust policy platform helps enterprises identify and protect sensitive data, monitor and control access to the data, and prevent regulatory violations – whether in the cloud or on premises. The software automates enforcement of security controls and compliance policies to enable secure information sharing across the extended enterprise. NextLabs has some of the largest global enterprises as customers and has strategic relationships with industry leaders such as SAP, Siemens, Microsoft, AWS, Accenture, Deloitte, Infosys, and IBM. For more information on NextLabs, please visit http://www.nextlabs.com.